PRE-APPEAL BRIEF REQUEST FOR REVIEW		Docket Number: TUC920010022US1
I hereby certify that this correspondence is being transmitted via the EFS-Web System to the USPTO on: September 24, 2009 Signature: /David Victor/ Typed or Printed Name: David W. Victor	**Application Number:** 09/977,159	**Filed:** October 11, 2001
	First Named Inventor: G.A. JAQUETTE	
	Art Unit: 3621	**Examiner:** Firmin Backer

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached five (5) sheet(s).
Note: No more than five (5) pages may be provided.

I am the:

☐ applicant/inventor

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

☒ attorney or agent of record.
Registration Number Registration No. 39,867

☐ attorney or agent acting under 37 CFR 1.34
Registration number if acting under 37 CFR 1.34

/David Victor/
Signature

David W. Victor
Typed or Printed Name

(310) 553-7977
Telephone Number

September 24, 2009
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required*.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	G.A. JAQUETTE	Examiner	Firmin Backer
Serial No.	09/977,159	Group Art Unit	3621
Filed	October 11, 2001	Docket No.	TUC920010022US1
TITLE	METHOD, SYSTEM, AND PROGRAM FOR SECURELY PROVIDING KEYS TO ENCODE AND DECODE DATA IN A STORAGE CARTRIDGE		

PRE-APPEAL BRIEF REQUEST FOR REVIEW ARGUMENTS

1. Sec. 101 Rejection: Applicants request review of the rejection of claims 1-16 and 44-46 as directed to non-statutory subject matter (35 U.S.C. §101) on the grounds that the claims are not tied to a statutory class nor transform underlying subject matter to a different state. (Final Office Action dated June 24, 2009 ("FOA"), pg. 2).

Applicants traverse because claim 1 recites that the operations are performed by a receiving interface device, which comprises a particular machine. Additionally, the claims recite the transformation of subject matter, in the form of the encrypted coding key which is read, transmitted, decrypted, received and used to code and decode data, all of which claimed operations involve the transformation of underlying subject matter, both the coding key and the data being coded and decoded. Accordingly, Applicants request that the Sec. 101 rejection of these claims be withdrawn.

2. Sec. 103 Rejection of Claims 1, 3-5, 7-16, and 44-75: Applicants request review of the rejection of the claims as obvious (35 U.S.C. §103(a)) over Shear (U.S. Patent Pub. 2001/0042043) in view of Smythe (U.S. Patent No. 5,325,430) and Levy (U.S. Patent No. 5,748,744).

a. Claims 1, 47, and 61: With respect to claim 1, 47, and 61, Applicants request review of the Examiner's finding that col. 3, lines 40-62 of Smythe teaches the claim requirement of receiving and decrypting, by the receiving interface device, the coding key encrypted by the host to use for the I/O request. (FOA, pg. 4) The cited col. 3 mentions a microprocessor connected via an encrypted address and data bus to a RAM, and the bus is encrypted using software logic within the microprocessor. The microprocessor includes an address encryptor and data encryptor, that both depend on an encryption key.

Although the cited Smythe discusses how a microprocessor encrypts data and addresses on a bus, the cited Smythe does not teach the specific claim requirements that an interface device receives and decrypts a coding key encrypted by a host to use for an I/O request. Instead, the

cited Smythe discusses how a microprocessor has an address and data encryptors to encrypt and decrypt data. There is no discussion in the cited Smythe of an interface device receiving and decrypting a coding key encrypted by a host, where the interface device previously transmitted the encrypted coding key to the host read from the cartridge.

The Examiner further found that the claim requirement "to code data to write to the target storage cartridge" represent non-functional descriptive information. (FOA, pg. 4) Applicants traverse this finding because the claim requirement "to code data" comprises an operation upon the data using a coding key to transform the data by the coding operation to write to the target storage cartridge. Such a functional coding operations is not non-functional descriptive.

Applicants further request review of the Examiner's finding that col. 5, line 54 to col. 6, line 3 and col. 6, lines 43-52 of Levy teach the claim requirements that the interface device read the encrypted coding key from a mounted storage cartridge, transmit the encrypted coding key to a host, and then receive the coding key encrypted by the host to decrypt and use. (FOA, pg. 5)

The cited cols. 5-6 discusses a Cipher Enable command that enables encrypted media using a hash derived from a user supplied keyphrase. The Cipher Enable command sets the media as an encrypted partition to appear to the user as a separate volume accessed with different logical unit numbers to distinguish from non-encrypted data. The cited col. 6 further mentions a command set to initialize a mass storage means to store encrypted data, allowing selection of a keyphrase during initialization of the storage, and allowing input of the keyphrase to unlock the key to access the encrypted data on the storage.

Although the cited cols. 5 and 6 of Levy discusses how to encrypt data on a storage using a user supplied keyphrase, there is no teaching of the claim requirements that the interface device read the encrypted coding key from a storage cartridge and transmit to a host, and then receive the coding key encrypted by the host, which the interface device then decrypts and uses. Instead, the cited Levy discusses how to use a user supplied keyphrase to decrypt data.

Thus, even if the references are combined as the Examiner proposes, the cited combination still does not teach or suggest the claim requirements for which the references were cited.

b. Claims 3, 48, 62: With respect to claims 3, 48, and 62, which depend from claims 1, 47, and 61, respectively, Applicants request review of the Examiner's finding that the above discussed FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220

of Shear teach the claim requirements that the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key encodes data written to the storage mediums and decode data read from the storage mediums of the plurality of storage cartridges. (FOA, pg. 6)

The cited para. 0078 discusses rights management to exchange movies and games. Content is encrypted with decryption keys required to decrypt the content. The decryption keys may themselves be encrypted in an encrypted key block. The cited para. 0079 mentions that content may be secured as it is recording, such as in a camera. Reading the content for use in the rights management environment might occur at many steps along a conventional production and distribution process. Para. 0080 mentions that the storage medium carries the decryption key in a hidden portion that is used by a drive to decrypt the encrypted key block. The cited para. 0081 mentions that the video disk drive may store keys to decrypt an encrypted key block or the may be stored in a drive key store and be updateable. The cited paras. 0127-0138 mention that different information on the medium may be encrypted using different keys and that encrypted keys may be stored on the medium to be used to decrypt the protected properties and metadata. Multiple sets of encrypted keys may be stored on the medium to have different keys associated with different regions. A decryption key for the encrypted keys may be hidden on the medium.

The cited para. 0183 mentions that a disk may store properties or other content in protected or unprotected form, where a property is protected if it is at least in part encrypted. The disk could store both a movie as protected property and an unprotected interview, and store any number of protected or unprotected properties. The cited paras. 0193-0199 discuss local secure execution of a control process and the use of optical media. Special hardware can be used to provide a secure execution environment to ensure safe digital commerce activities. A metering and control system, at least partially encrypted, is delivered to a user on optical media. A bill may be generated in response to transmitting information. Some or all of the content may be encrypted on the media. The cited paras. 0216-0220 further discusses that the disk may store an encrypted key block used to decrypt properties and metadata on the disk, where different keys may be used for different data on the disk. The cited para. [0217] mentions that the cryptographic key block, which is the key used to decrypt the data, may be encrypted with one or more additional keys, and that these one or more keys need to be used to decrypt the key block to obtain the key to decrypt the data. The cited paras. [0218-0220] mentions that the keys to decrypt the encrypted key block may come from different sources. The disk may store hidden

keys or the keys may be provided by the disk drive. The disk drive may have an integrated circuit decryption engine including a small secure internal key store memory having keys to use to decrypt the encrypted key block, which is then used to decrypt the content. The keys to decrypt the protected content may also be within a secure container.

The above cited Sheer discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys. Although the cited Sheer discusses encrypting a decrypting key block used to decrypt content on the disk with one or more keys, the Examiner has not cited any part of Shear that teaches that one key is associated with a plurality of storage cartridges, wherein this one key is used to code and decode data from the storage mediums of the storage cartridges.

c. Claims 7, 50, and 65: With respect to claims 7, 50, and 65, which depend from claims 1, 47, and 61, Applicants request review of the Examiner's findings that FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear teach the claim requirement encrypting the coding key comprising encrypting, by the host (or I/O manager in the case of claim 65), the coding key with a first key, wherein the interface devices use a second key to decrypt the coding key encrypted with the first key.

As discussed, the above cited Sheer discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. Although the cited Sheer discusses encrypting a decrypting key block used to decrypt content on the disk with one or more keys, the Examiner has not cited any part of Shear that teaches encrypting the coding key with a first key, where the host uses a second key to decrypt the coding key, and that the host encrypts the coding key with a third key, and that the interface device, or cited drive, uses a fourth key the key that is then used to decrypt the coding key, or cited encrypted key block.

d. Claims 10, 54, and 68: Applicants request review of the Examiner's findings that the above cited paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear teach the requirements of claims 10, 54, and 68. (FOA, pg. 9)

In particular, Applicants submit that the Examiner has not cited any part of Shear that teaches or suggests an interface device for accessing a coupled storage medium receive an encrypted coding key from a host with an I/O request directed to the storage cartridge, mounting the storage cartridge in response to the received I/O request, decrypting the encrypted coding key, and using the coding key to encode data to write to the storage medium for a write I/O request and decode data read from the storage for a read I/O request. Instead, as discussed, the cited Shear discusses a drive accessing an encrypted decrypting key to use to decrypt content on a disk (DVD).

Further, the Examiner has not cited any part of Shear that teaches the claim requirement of storing the received encrypted coding key in the storage medium to use for subsequent I/O requests. The above cited Sheer discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. However, the cited sections do not teach that the disk drive, which decrypted and used a key to code data to write to the storage, stores an encrypted coding key received from a host system with an I/O request in the storage medium for subsequent I/O requests.

e. Claims 16, 59, 74: With respect to these claims, Applicants request review of the Examiner's findings that the above discussed Shear teaches the claim requirements. (FOA, pg. 10)

Applicants submit that the Examiner has not cited any part of Shear that teaches that the coding key, corresponding to the cited decryption key, is encrypted with a first key and that the interface device receives a second key encrypted with a third key that it decrypts with a fourth key to then use the second key to decrypt encrypted coding key to use. For instance, the Examiner has not cited where Shear discloses that the disk drive receives a further key that is used to decrypt the key it maintains to use to decrypt the key block on the DVD. Instead, the cited Shear, including para. 0217 mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys.

Dated: September 24, 2009

By: /David Victor/
David W. Victor
Registration No. 39,867
Tel: (310) 553-7977